CLAIMS

We claim:

1. A method of blocking attacks on a computer network, comprising:
receiving original packets and corresponding retransmit packets from a network, wherein:
each said original packet and corresponding retransmit packet belong to a flow; and
each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;
hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;
storing said validation signatures;
hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;
comparing said validation signature to said test signature; and
if said test signature and said validation signature are not identical, terminating said flow.

2. The method of Claim 1, wherein said storing comprises retaining said validation signatures for a limited time.

3. The method of Claim 1, wherein said hashing comprises computing a checksum from said non-mutable field values.

4. The method of Claim 1, wherein said hashing comprises computing a hash value from said non-mutable field values.

5. The method of Claim 1, wherein said hashing comprises computing a strong hash value from said non-mutable field values.

6. The method of Claim 1, wherein said hashing comprises computing a cryptographically secure hash value from said non-mutable field values.

7. The method of Claim 1, wherein said hashing comprises computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

8. The method of Claim 1, wherein said hashing comprises computing a hash value using a secret number.

9. A method of blocking attacks on a computer network, comprising:
generating a validation signature of an original packet;
generating a test signature of a retransmit packet, said retransmit packet being a retransmission of said original packet with a flow of packets; and
comparing said test signature to said validation signature to determine whether to terminate said flow of packets.

10. An apparatus for blocking attacks on a computer network, comprising:
means for receiving original packets and corresponding retransmit packets from a network, wherein:
each said original packet and corresponding retransmit packet belong to a flow; and
each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;
first means for hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;
means for storing said validation signatures;
second means for hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet, wherein said first means for hashing and said second means for hashing employ the same hashing algorithm;
means for comparing said validation signature to said test signature; and

means for terminating said flow if said test signature and said validation signature are not identical.

11. The apparatus of Claim 10, wherein said means for storing comprises means for retaining said validation signatures for a limited time.

12. The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a checksum from said non-mutable field values.

13. The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a hash value from said non-mutable field values.

14. The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a strong hash value from said non-mutable field values.

15. The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a cryptographically secure hash value from said non-mutable field values.

16. The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

17. The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a hash value using a secret number.

18. An apparatus for blocking attacks on a computer network, comprising:

a packet hashing device configured to receive original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow;

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values; and

said packet hashing device employing a packet hashing algorithm to hash said non-mutable field values of each said original packet to produce a validation signature of each said original packet and to hash said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

a flow cache connected to said packet hashing device and configured to store said validation signatures;

a comparator operably connected to said flow cache configured to compare said validation signature to said test signature and having an output; and

a flow terminator receiving said output of said comparator and configured to terminate said flow if said output indicates that said test signature and said validation signature are not identical.

19. The apparatus of Claim 18, wherein said flow cache comprises means for retaining said validation signatures for a limited time.

20. The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a checksum from said non-mutable field values.

21. The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a hash value from said non-mutable field values.

22. The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a strong hash value from said non-mutable field values.

23. The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a cryptographically secure hash value from said non-mutable field values.

24. The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

25. The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a hash value using a secret number.

26. A computer system for use in blocking attacks on a computer network, comprising computer instructions for:

receiving original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow; and

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;

hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;

storing said validation signatures;

hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

comparing said validation signature to said test signature; and

if said test signature and said validation signature are not identical, terminating said flow.

27. The computer system of Claim 26, wherein said computer instructions for storing further comprise computer instructions for retaining said validation signatures for a limited time.

28. The computer system of Claim 26, wherein said computer instructions for hashing further comprise computer instructions for computing a checksum from said non-mutable field values.

29. The computer system of Claim 26, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value from said non-mutable field values.

30. The computer system of Claim 26, wherein said computer instructions for hashing further comprise computer instructions for computing a strong hash value from said non-mutable field values.

31. The computer system of Claim 26, wherein said computer instructions for hashing further comprise computer instructions for computing a cryptographically secure hash value from said non-mutable field values.

32. The computer system of Claim 26, wherein said computer instructions for hashing further comprise computer instructions for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

33. The computer system of Claim 26, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value using a secret number.

34. A computer-readable medium storing a computer program executable by a plurality of server computers, the computer program comprising computer instructions for:

receiving original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow; and

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;

hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;

storing said validation signatures;

hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

comparing said validation signature to said test signature; and

if said test signature and said validation signature are not identical, terminating said flow.

35. The computer-readable medium of Claim 34, wherein said computer instructions for storing further comprise computer instructions for retaining said validation signatures for a limited time.

36. The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a checksum from said non-mutable field values.

37. The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value from said non-mutable field values.

38. The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a strong hash value from said non-mutable field values.

39. The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a cryptographically secure hash value from said non-mutable field values.

40. The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

41. The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value using a secret number.

42. A computer data signal embodied in a carrier wave, comprising computer instructions for:

receiving original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow; and

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;

hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;

storing said validation signatures;

hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

comparing said validation signature to said test signature; and

if said test signature and said validation signature are not identical, terminating said flow.

43. The computer data signal of Claim 42, wherein said computer instructions storing further comprise computer instructions for retaining said validation signatures for a limited time.

44. The computer data signal of Claim 42, wherein computer instructions for hashing further comprise computer instructions for computing a checksum from said non-mutable field values.

45. The computer data signal of Claim 42, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value from said non-mutable field values.

46. The computer data signal of Claim 42, wherein said computer instructions for hashing further comprise computer instructions for computing a strong hash value from said non-mutable field values.

47. The computer data signal of Claim 42, wherein said computer instructions for hashing further comprise computer instructions for computing a cryptographically secure hash value from said non-mutable field values.

48. The computer data signal of Claim 42, wherein said computer instructions for hashing further comprise computer instructions for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

49. The computer data signal of Claim 42, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value using a secret number.